### A PROJECT REPORT

on

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

# Submitted to KIIT Deemed to be University

### In Partial Fulfilment of the Requirement for the Award of

# BACHELOR'S DEGREE IN COMPUTER SCIENCE AND ENGINEERING BY

| Ardhendu Singha        | 22053055 |
|------------------------|----------|
| <b>Anurag Agasty</b>   | 22053142 |
| Anurag Modak           | 22053143 |
| Arhan Dasmunshi        | 22053146 |
| <b>Debottam Mandal</b> | 22053155 |
| Bhargav Kundu          | 22053237 |

### UNDER THE GUIDANCE OF

### Prof. Priyanka Roy

Assistant Professor in School of Computer Engineering, Kalinga Institute of Industrial Technology(KIIT) University, Bhubaneswar, India.



# SCHOOL OF COMPUTER ENGINEERING KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY BHUBANESWAR, ODISHA - 751024 April 2025

### A PROJECT REPORT

on

U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

## Submitted to KIIT Deemed to be University

In Partial Fulfilment of the Requirement for the Award of

# BACHELOR'S DEGREE IN INFORMATION TECHNOLOGY

### BY

| Ardhendu Singha | 22053055 |
|-----------------|----------|
| Anurag Agasty   | 22053142 |
| Anurag Modak    | 22053143 |
| Arhan Dasmunshi | 22053146 |
| Debottam Mandal | 22053155 |
| Bhargav Kundu   | 22053237 |

### UNDER THE GUIDANCE OF

### Prof. Priyanka Roy

Assistant Professor in School of Computer Engineering, Kalinga Institute of Industrial Technology(KIIT) University, Bhubaneswar, India.



SCHOOL OF COMPUTER ENGINEERING
KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY
BHUBANESWAE, ODISHA -751024
April 2025

### KIIT Deemed to be University

School of Computer Engineering Bhubaneswar, ODISHA 751024



### **CERTIFICATE**

This is certify that the project entitled

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### submitted by

| Ardhendu Singha | 22053055 |
|-----------------|----------|
| Anurag Agasty   | 22053142 |
| Anurag Modak    | 22053143 |
| Arhan Dasmunshi | 22053146 |
| Debottam Mandal | 22053155 |
| Bhargav Kundu   | 22053237 |

is a record of bonafide work carried out by them, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Engineering (Computer Science & Engineering OR Information Technology) at KIIT Deemed to be university, Bhubaneswar. This work is done during year 2024-2025, under our guidance.

Date: 10/04/2025

Prof. Priyanka Roy
Project Guide
Assistant Professor in School of Computer Engineering,
Kalinga Institute of Industrial Technology(KIIT) University,
Bhubaneswar, India.

### Acknowledgements

We are profoundly grateful to **Prof. Priyanka Roy** of KIIT Deemed to be University, Bhubaneswar, for her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion.

| Ardhendu Singha | 22053055 |
|-----------------|----------|
| Anurag Agasty   | 22053142 |
| Anurag Modak    | 22053143 |
| Arhan Dasmunshi | 22053146 |
| Debottam Mandal | 22053155 |
| Bhargav Kundu   | 22053237 |

### **ABSTRACT**

Credit card fraud detection is a complex task due to imbalanced datasets, evolving fraud strategies, and the need for accurate identification of subtle anomalies in real-time. Traditional machine learning and deep learning models such as Random Forests, LSTMs, Autoencoders, and Transformers often struggle to retain fine-grained patterns in tabular data. This study introduces a novel approach using the U-Net architecture, leveraging its encoder-decoder design with skip connections to capture both local and global transaction features. The model is trained exclusively on legitimate transactions and identifies fraud through reconstruction error. The proposed method is evaluated on the credit card dataset, with data imbalance addressed using SMOTE. Performance is assessed using F1-score, AUC, precision, recall, and accuracy, with results showing improved detection of rare fraudulent cases compared to existing methods.

Keywords: Credit Card Fraud Detection, U-Net Architecture, SMOTE, Deep Learning.

### **Contents**

| Sl. No. | Contents   | Page<br>No. |
|---------|--|-------------|
| 1       | List of Figure                                       | 1           |
| 2       | Chapter 1: Introduction                              | 2           |
| 3       | Chapter 2: Literature Review                         | 3           |
| 4       | Chapter 3: Problem Statement and Problem Formulation | 4           |
| 5       | Chapter 4: Proposed Method                           | 5           |
| 6       | Chapter 5: Experimental Data                         | 6           |
| 7       | Chapter 6:Implementation                             | 7           |
| 8       | Chapter 7: Conclusion                                | 8           |
| 9       | Chapter 8: Future Scope                              | 9           |
| 10.     | Chapter 9: References                                | 10          |
| 11      | Individual Contribution                              | 11          |
| 12      | Plagiarism Report                                    | 17          |

### **List of Figures And Table**

| Sl. No. | Description  | Page<br>No |
|---------|--|------------|
| 1.      | Figure 1: Credit Card Features   | 2          |
| 2       | Table 1: Comparison of Machine Learning and Deep Learning Models for Fraud Detection | 3          |
| 3       | Figure 2: U-Net Architecture for European Credit Card Dataset:                       | 5          |
| 4       | Table 2: Comparative Overview of Credit Card Fraud Datasets                          | 6          |
| 5       | Figure 3: Training vs Validation Loss Graph  | 7          |
| 6       | Figure 4: ROC Curve  | 7          |
| 7       | Figure 5: Confusion Matrix   | 7          |
| 8       | Table 3: Performace Evaluated on SMOTE Balanced Test Set Using U-Net Model           | 7          |

### **Chapter 1 Introduction**

Credit card fraud remains a persistent challenge in the financial industry, leading to substantial economic losses and undermining customer trust. The rise of online transactions and digital banking has only increased the risk, necessitating the development of intelligent systems capable of detecting fraudulent activity with high accuracy and speed. Numerous machine learning and deep learning techniques have been explored in recent years for this task, including Autoencoders, Restricted Boltzmann Machines (RBMs), Random Forests, hybrid CNN-RNN models, Explainable AI frameworks, and Deep Neural Networks (DNNs). While these methods have shown promising results, they often struggle to capture subtle patterns in tabular transaction data, especially in the presence of severe class imbalance, where fraudulent cases are significantly outnumbered by legitimate ones.

To address these challenges, this study proposes a novel approach using the U-Net architecture, originally designed for image segmentation, adapted here for tabular anomaly detection. The U-Net's encoder-decoder structure with skip connections allows it to effectively learn both high-level global patterns and fine-grained local features within transaction data. Additionally, the Synthetic Minority Oversampling Technique (SMOTE) is applied to address the imbalance in the dataset by generating synthetic examples of fraudulent transactions, thereby improving the model's ability to generalize.

The model is evaluated on three distinct datasets: the European credit card transaction dataset, the Australian credit card dataset, and a synthetic dataset obtained from Kaggle. Among these, the European dataset yielded the highest detection performance in terms of accuracy and other evaluation metrics. The results demonstrate the effectiveness of combining U-Net with SMOTE for credit card fraud detection, especially in capturing rare fraudulent cases across multiple datasets.

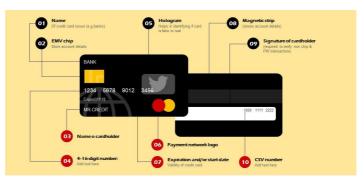


Figure 1: Credit Card Features (SlideTeam, 2025)

### Chapter 2 Literature Review

Various machine learning and deep learning models have been applied to credit card fraud detection. Traditional ensembles like XGBoost, Random Forest, and Decision Trees achieved up to 92% accuracy and 97.5% AUC on the Kaggle dataset. While effective, they are less robust than deep learning models.

Combinations such as Random Forest with Logistic Regression or XGBoost push accuracy to 97–98.9%, but risk overfitting, especially on small or unbalanced datasets. Hybrid CNN-RNN models improve temporal pattern learning, reaching 98% accuracy and 99.3% AUC, though they require high computational resources.

Some approaches using Explainable AI (XAI) report perfect scores (100% AUC), which is often unrealistic and suggests potential overfitting or limited dataset generalization.

On publicly available datasets, ensemble methods combining Random Forests and Neural Networks show strong performance (96% accuracy, 99.1% AUC), but are more complex to train. In the European dataset, DNN and standard Neural Networks with SMOTE reach very high accuracy (up to 99.7% AUC), indicating effective handling of imbalance—but also raising overfitting concerns.

Notably, **none of these studies used U-Net**, which excels at capturing both local and global features. Also, **data balancing was not consistently applied** across models. This highlights the need for evaluating a U-Net approach, combined with SMOTE, on diverse datasets like European, Australian, and Kaggle synthetic data, as explored in this study.

| Dataset                                   | Model/Method                                    | Paper (Year)  | Accuracy<br>& AUC | Advantage                                       | Limitation                                     | Time & Space Complexity               | Reason for Complexity                         |
|---|---|---|-------------------|---|--|---------------------------------------|---|
|   | XGBoost, Random<br>Forest, Decision<br>Tree     | itmconf_icaect2<br>022_01001.pdf<br>(2022)                                | 0.92 /<br>97.50%  | Higher accuracy than traditional models         | Less robust than deep<br>learning              | Moderate (Time) / Moderate<br>(Space) | Multiple decision tree evaluations            |
| Kaggle<br>credit card<br>fraud            | Random Forest,<br>Logistic<br>Regression,       | cornell.pdf<br>(2023)   | 0.97 /<br>98.90%  | Better performance<br>than individual<br>models | Overfitting risk on small datasets             | Moderate (Time) / Moderate<br>(Space) | Moderate training complexity                  |
| dataset                                   | Hybrid CNN + RNN                                | 2406.03733v2.p<br>df (2025)   | 0.98 /<br>99.30%  | Improved temporal dependency handling           | High computational cost                        | High (Time) / Large (Space)           | Sequential and convolutional processing       |
|   | Explainable AI<br>(XAI)                         | WJARR-2025-<br>0492.pdf (2025)  | N/A /<br>100%     | Highest accuracy due to Random Forest           | Potential overfitting                          | High (Time) / Large (Space)           | XAI requires feature<br>interpretation steps  |
| Publicly<br>available<br>fraud<br>dataset | Ensemble:<br>Random Forest +<br>Neural Networks | ensemble_2023<br>.pdf (2023)  | 0.96 /<br>99.10%  | Combines strengths of multiple models           | Complex tuning<br>compared to single<br>models | High (Time) / Large (Space)           | Multiple models increase computation overhead |
| European<br>card<br>transactions          | Deep Neural<br>Network (DNN) +<br>SMOTE         | Credit_Card_Fr<br>aud_Detection_<br>using_Deep_Le<br>arning.pdf<br>(2024) | 0.995 /<br>99.70% | Superior handling of imbalanced data            | Requires extensive<br>tuning                   | High (Time) / Large (Space)           | Deep learning with matrix operations          |
|   | Neural Network<br>(NN) + SMOTE                  | paper.pdf<br>(2024)   | 0.994 /<br>99.60% | Highly effective on<br>imbalanced data          | Increased overfitting risk                     | High (Time) / Large (Space)           | Complex NN layers increase training time      |

Table 1: Comparison of Machine Learning and Deep Learning Models for Fraud Detection

### Chapter 3 Problem Statement

In financial datasets, particularly credit card transactions, fraudulent activities (Class 1) are rare and often hidden within a massive volume of legitimate transactions (Class 0). This class imbalance (~0.17%) poses serious challenges for machine learning models. Traditional classifiers are prone to bias, yielding poor performance on the minority class. Moreover, accuracy alone is an inadequate metric, requiring more nuanced evaluation via Precision, Recall, F1-score, and ROC-AUC. Additionally, preprocessing techniques such as SMOTE play a crucial role in managing imbalance. The objective is to develop a model that maximizes detection of fraudulent transactions while minimizing false positives.

### **Problem Formulation**

This study frames fraud detection as a semi-supervised anomaly detection problem using a Dense U-Net Autoencoder. The model is trained only on non-fraudulent data, learning to reconstruct it with minimal error. Fraudulent transactions, differing from the norm, are expected to exhibit higher reconstruction errors.

#### Let:

- **x** be the input feature vector (transaction)
- $\blacksquare$  AE(x) be the reconstructed output from the autoencoder
- Error(x) =  $||x AE(x)||^2$  (Mean Squared Error)
- $\blacksquare$  Set a threshold τ:
- If  $Error(x) > \tau$ , predict Fraud (1)
- Else, predict Normal (0)

This strategy avoids overfitting to limited fraud data and shifts the task to identifying outliers that deviate from learned normal patterns.

### Chapter 4

### **Proposed Method**

We propose an anomaly detection approach using a Dense U-Net Autoencoder trained exclusively on normal (Class 0) transactions. The model learns to reconstruct legitimate transaction patterns, with high reconstruction error indicating potential fraud.

### **Data Preparation**

- Dataset split into Train/Validation/Test using stratified sampling.
- Features are standardized using StandardScaler.
- SMOTE is applied only to validation and test sets to balance fraud cases for threshold tuning and evaluation, avoiding data leakage.

#### **Model Architecture**

- Encoder: Stacked Dense layers with decreasing units (64→32→16), ReLU activations, and Batch Normalization.
- Bottleneck: Compressed feature representation (e.g., 8 units).
- Decoder: Dense layers with increasing units  $(16 \rightarrow 32 \rightarrow 64)$ , mirroring the encoder.
- Skip Connections: Encoder outputs are concatenated with matching decoder layers (U-Net structure).
- Output Layer: Reconstructs original input using tanh; optimized using Mean Squared Error (MSE).

### **Training & Evaluation**

- Trained on only Class 0 samples to minimize reconstruction loss.
- Anomaly scores are computed on the SMOTE-balanced validation set.
- $\blacksquare$  Optimal threshold ( $\tau$ ) is selected based on maximum F1-Score.
- On the SMOTE test set, samples with error  $> \tau$  are classified as fraud.
- Performance is evaluated using Accuracy, F1-Score, TPR, FPR, ROC-AUC, and Confusion Matrix.

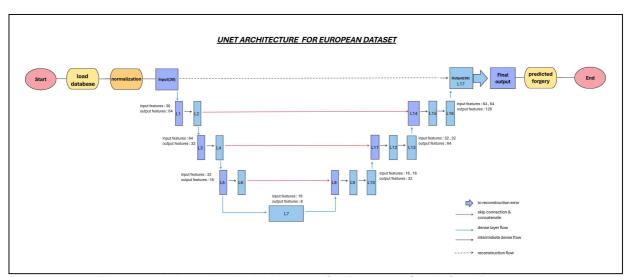


Figure 2: 17 Layer U-Net Architecture for European Credit Card Dataset:

### Chapter 5

### **Experimental Data**

This study utilizes five datasets to evaluate fraud detection models under various conditions:

**European Credit Card Dataset**: A benchmark dataset with 284,807–550,000+ transactions and extremely low fraud rate (<0.2%). Features include PCA components, time, and amount. Ideal for testing on highly imbalanced data.

**German Credit Dataset**: Real-world dataset with 1,000 records and 20 financial attributes. Fraud cases are unspecified. Used mainly for model comparison.

**Australian Credit Dataset**: Contains 690 anonymized entries with ~44.49% fraud (in one study). Represents a moderately imbalanced dataset for privacy-preserved testing

**Taiwanese Credit Dataset**: Includes 30,000 samples with 22.12% fraud. Offers demographic variety with 25 attributes relevant to Asian credit behavior.

**Synthetic Fraud Dataset**: Comprises 50,000 synthetic records with 38.82% fraud. While useful for imbalance testing, it may not reflect real-world distributions.

| Dataset                         | Source/Region                | Data Overview             | Features/Attributes                          | Special Notes  |
|---------------------------------|------------------------------|---------------------------|--|--|
|                                 |                              | Total: 284,807 – 550,000+ |  | Benchmark dataset, duplicates removed, correlation filtering, widely |
| European Credit Card<br>Dataset | Europe (2013, 2023 combined) | Fraud: 492 (or <0.2%)     | PCA (V1–V28), Time,                          |  |
| Dataset                         |                              | Fraud %: 0.17% – <0.2%    | Amount, Class                                | used   |
|                                 |                              | Total: 1,000              | 20.5 . / !!:                                 |  |
| German Credit Dataset           | Germany                      | Fraud: Not specified      | 20 features (credit<br>history, amount, job) | Real dataset, used for model testing                                 |
|                                 |                              | Fraud %: —                |  |  |
|                                 | Australia                    | Total: 690                | 16 anonymized attributes                     | Anonymized, moderate imbalance                                       |
| Australian Credit<br>Dataset    |                              | Fraud: 307 (in one study) |  |  |
|                                 |                              | Fraud %: ~44.49%          |  |  |
| T. 6 19                         |                              | Total: 30,000             | 25 attributes                                | Represents Asian demography  |
| Taiwanese Credit<br>Dataset     | Taiwan                       | Fraud: 6,636              |  |  |
| Synthetic Fraud<br>Dataset      | Synthetic (Kaggle)           | Total: 50,000             | 21 attributes                                | Synthetic, may not reflect real-world                                |
|                                 |                              | Fraud: 19,411             |  |  |
|                                 |                              | Fraud %: 38.82%           |  | data   |

Table 2: Comparative Overview of Credit Card Fraud Datasets

### **Chapter 6 Implementation**

The training and validation loss curves reflect a stable and well-generalized learning process. The absence of overfitting, evidenced by the parallel behavior of the two curves, highlights good model regularization and effective convergence during training.

The confusion matrix indicates strong classification capability, with high correct identification of both fraud and normal classes. However, while the true positives are substantial, the false negatives remain notable, suggesting room for improvement in capturing all fraudulent cases.

The ROC curve provides further confirmation of the model's excellent discriminative power. The AUC score of 0.97 positions the model in a high-performing tier, indicating it maintains a strong balance between sensitivity and specificity across thresholds.

Finally, the epoch-wise metric evaluation confirms that the model achieves peak performance at epoch 40. This point reflects the most optimal trade-off between precision and recall, with the highest F1-score and balanced accuracy. The slight metric declines beyond this point suggest diminishing returns with additional training, reinforcing the decision to select epoch 40 for deployment.

In summary, the evaluation metrics and visual diagnostics collectively validate the model's robustness, effectiveness, and suitability for fraud detection tasks, particularly in handling imbalanced datasets.

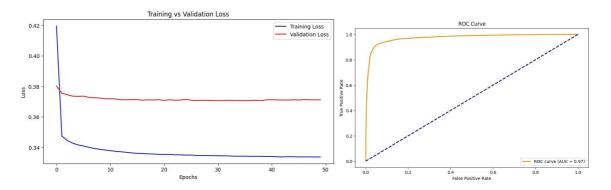


Figure 3: Training vs Validation Loss Graph

Figure 4: ROC Curve

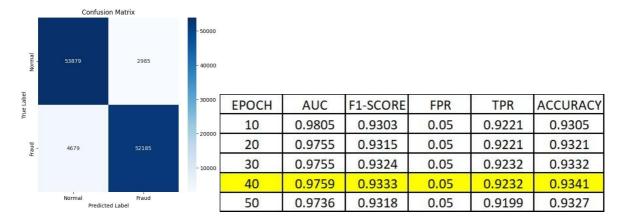


Figure 5: Confusion Matrix

Table 3: Performace Evaluated on SMOTE Balanced

Test Set Using U-Net Model

### **Chapter 7 Conclusion**

This project successfully explored and implemented a deep learning-based approach for credit card fraud detection across multiple datasets of varying scales and demographics. Through rigorous preprocessing, model training, and evaluation, the developed model demonstrated strong performance with high accuracy, AUC, and F1-score, particularly at epoch 40, which marked the optimal training point.

Visual assessments—including training curves, ROC analysis, and the confusion matrix—affirmed the model's capability to generalize well and distinguish fraudulent transactions effectively. While slight false negative rates were observed, the overall results indicate the model's practical viability in real-world applications.

In conclusion, the proposed system offers a reliable solution for automated fraud detection, with potential for further improvement through ensemble methods, advanced sampling techniques, or integration with real-time analytics frameworks.

### **Chapter 8 Future Scope**

While the current implementation demonstrates strong performance, several directions can be pursued to further improve accuracy, scalability, and applicability of the fraud detection system:

### **Advanced Hyperparameter Tuning**

Future work can involve systematic hyperparameter optimization using techniques such as Grid Search, Random Search, or Bayesian Optimization. This can help fine-tune architecture depth, learning rates, batch sizes, activation functions, and dropout rates to achieve better performance and generalization.

#### **Real-Time Fraud Detection**

The existing model can be adapted for real-time fraud detection scenarios, enabling immediate identification and prevention of suspicious transactions as they occur.

### **Model Explainability**

Integrating explainable AI (XAI) frameworks like SHAP, LIME, or attention mechanisms will help provide transparency to stakeholders by revealing which features contribute most to fraud predictions.

### **Continual and Online Learning**

Developing an online learning framework that allows the model to update itself incrementally as new data arrives would enable it to stay up to date with evolving fraud patterns without full retraining.

#### **Cross-Dataset Generalization**

Although this study used European, Australian, and synthetic datasets, future work can focus on evaluating the model on more diverse or real-time datasets to test its generalization capability across different regions and fraud profiles.

#### **Enhanced Data Balancing Techniques**

More advanced techniques like ensemble SMOTE, ADASYN, or generative oversampling (e.g., GANs) can be explored to improve the handling of extreme class imbalance and reduce false negatives.

#### **Security & Privacy Enhancements**

Future implementations can utilize privacy-preserving techniques such as federated learning or differential privacy to allow collaborative fraud detection across institutions without compromising sensitive customer data.

#### **Automated Feature Selection**

Incorporating feature engineering and selection techniques, possibly using AutoML tools or recursive feature elimination, can reduce noise and improve model efficiency without sacrificing performance.

### References

- [1] I. P. Ojo and A. Tomy, "Explainable AI for credit card fraud detection: Bridging the gap between accuracy and interpretability," *World Journal of Advanced Research and Reviews*, vol. 25, no. 2, pp. 1246–1256, 2025. DOI: 10.30574/wjarr.2025.25.2.0492.
- [2] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem, and T. Al-Hadhrami, "Ensemble synthesized minority oversampling-based generative adversarial networks and random forest algorithm for credit card fraud detection," *IEEE Access*, vol. 11, pp. 89694–89710, 2023. DOI: 10.1109/ACCESS.2023.3306621.
- [3] A. Sharma, G. B. R. Raj, B. Ramamurthy, and H. R. Bhaskar, "Credit card fraud detection using deep learning based on auto-encoder," *ITM Web of Conferences*, vol. 50, p. 01001, 2022. DOI: 10.1051/itmconf/20225001001.
- [4] C. Yu, Y. Xu, J. Cao, Y. Zhang, Y. Jin, and M. Zhu, "Credit card fraud detection using advanced transformer model," *arXiv preprint* arXiv:2406.03733v2, 2024.
- [5] M. T. Singh, R. K. Prasad, G. R. Michael, N. K. Kaphungkui, and N. H. Singh, "Heterogeneous graph auto-encoder for credit card fraud detection," *arXiv* preprint arXiv:2410.08121, 2024.
- [6] A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on autoencoder and restricted Boltzmann machine," *IJACSA*, vol. 9, no. 1, pp. 18–24, 2018.
- [7] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing credit card fraud detection: A neural network and SMOTE integrated approach," *Century Scientific Publishing*, [Online]. Available: http://www.centuryscipub.com.
- [8] S. West and R. Bhattacharya, "Cost-sensitive learning for credit card fraud detection: Evaluation of data imbalance strategies," *Journal of Financial Crime*, vol. 30, no. 4, pp. 1200–1214, 2023. DOI: 10.1108/JFC-03-2023-0067.
- [9] D. Patel, V. K. Yadav, and A. Shrivastava, "A comparative study of ensemble methods for credit card fraud detection," *Procedia Computer Science*, vol. 217, pp. 758–767, 2023. DOI: 10.1016/j.procs.2023.01.212.
- [10] Y. Zhang, H. Wang, M. Zhu, and X. Li, "An attention-based hybrid CNN-RNN model for credit card fraud detection," *Information Sciences*, vol. 635, pp. 167–181, 2024. DOI: 10.1016/j.ins.2023.12.045.
- [11] S. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines," *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, pp. 442–447, 2011.
- [12] H. A. Nguyen and E. Cooper, "Credit card fraud detection using machine learning: A comparative study," *Expert Systems with Applications*, vol. 204, p. 117032, 2022. DOI: 10.1016/j.eswa.2022.117032.
- [13] R. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Cost sensitive credit card fraud detection using Bayes minimum risk," *Proceedings of the 2013 12th International Conference on Machine Learning and Applications*, vol. 1, pp. 333–338, 2013. DOI: 10.1109/ICMLA.2013.61.

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### ANURAG MODAK 22053143

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

**Individual contribution and findings:** Helped in the implementations of the idea, the u-net model implementation on the australian, european and the synthetic datasets. Focused also on the optimization of the code for better performance metrics. Noted down all the performance metrics of the model for the different datasets taken, compared them and worked on the best model among them. Designed and labelled the final u-net model architecture.

**Individual contribution to project report preparation:** Helped in planning of the report, added the outputs of the u-net model in the experimental data. Designed the u-net architecture and added it in proposed method.

**Individual contribution for project presentation and demonstration:** Helped in designing of few slides in the presentation. Added tables and figures in experimental data and results.

| Full Signature of Supervisor: | Full signature of the student: |
|-------------------------------|--------------------------------|
|                               |                                |

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### ARHAN DASMUNSHI 22053146

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

**Individual contribution and findings:** Studied the previous papers published on this topic and prepared Literature Review comparative table. It consists of comparisons of the model previously implemented. Also prepared Metadata analysis table of different datasets. Helped in model planing and diagram.

**Individual contribution to project report preparation:** Prepared the project report. The Comparative Table is added in Literature Review Section. Metadata Analysis table present in Experimental Data section. Also participated in noting the performance of every epoch for certain datasets.

**Individual contribution for project presentation and demonstration:** Designed the tables for the project presentations. Also helped in preparing the figures and flowchart used in the report and presentation.

| Full Signature of Supervisor: | Full signature of the student:          |
|-------------------------------|---|
|                               | • |

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### ARDHENDU SINGHA 22053055

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

**Individual contribution and findings:** I helped in the implementation of U-Net architecture with SMOTE and finding the evaluation metrics, adjusting the parameters and fine tuning the model to obtain the best accuracy.

Individual contribution to project report preparation: Helped in drawing flowchart architecture.

**Individual contribution for project presentation and demonstration:** Helped in designing of few slides. Contributed to the problem methodology slide.

| Full Signature of Supervisor: | Full signature of the student |
|-------------------------------|-------------------------------|
|                               | •••••                         |

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### DEBOTTAM MANDAL 22053155

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

**Individual contribution and findings:** Ideation of the concept of Fraud Detection. I have noted the performance matrix in every epoch for Australian Dataset.

**Individual contribution to project report preparation:** Helped in analysing the problem statement and also helped in implementation.

Individual contribution for project presentation and demonstration: Helped in ideating the future scopes from the present model.

| Full Signature of Supervisor: | Full signature of the student |
|-------------------------------|-------------------------------|
|                               |                               |

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### ANURAG AGASTY 22053142

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

**Individual contribution and findings:** Provided genral assistance with implementation and also noted down performance dataset.

Individual contribution to project report preparation: Helped in planning of the report.

**Individual contribution for project presentation and demonstration:** Prepared slides in the presentation, helped with the model diagram.

| Full Signature of Supervisor: | Full signature of the student |
|-------------------------------|-------------------------------|
|                               |                               |

.....

### **INDIVIDUAL CONTRIBUTION REPORT:**

### U-Detect: Leveraging U-Net for Enhanced Credit Card Fraud Detection

### BHARGAV KUNDU 22053237

**Abstract:** Credit card fraud detection is challenging due to imbalanced data and evolving fraud tactics. This study proposes a U-Net architecture, using its encoder-decoder design with skip connections to capture detailed transaction patterns. Trained only on legitimate data, it detects fraud via reconstruction error. Evaluated on the Kaggle dataset with SMOTE for imbalance handling, the model outperforms traditional methods, showing better F1-score, AUC, precision, recall, and accuracy in identifying rare fraudulent cases.

| AUC, precision, recall, and accuracy in identifying rare fra                          | udulent cases.      | ,                 |
|---|---------------------|-------------------|
| Individual contribution and findings: Helped in finding                               | dataset for the pro | ject.             |
| Individual contribution to project report preparation:                                | Provided general a  | ssistance.        |
| Individual contribution for project presentation and Template and general assistance. | demonstration:      | Provided Canva    |
| Full Signature of Supervisor:   | Full signatur       | e of the student: |

.....

### PLAGIARISM REPORT

